

Fault-Tolerant Guidance Algorithms for Cassini's Saturn Orbit Insertion Burn

Donald L. Gray and G. Mark Brown

Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California

Abstract

This paper describes a strategy that provides maximum assurance that Cassini's Saturn orbit insertion (SOI) will be successful. First the criticality of the SOI to the mission is shown and how it reduces to an energy only correction. Then autonomous on-board diagnostic and response algorithms are described that respond to any combination of problems that might be encountered during the burn. An accurate restart algorithm is implemented to complete the energy correction if at all possible.

Nominal SOI Strategy

The Saturn Orbit Insertion (SOI) is arguably the most critical single maneuver in the entire Cassini mission. It is used to reduce the spacecraft's incoming energy from an interplanetary flyby and place it into a trajectory about Saturn with a desired orbit period (currently 146 days). Since it is an energy reducing maneuver it is ideally performed opposite to the spacecraft velocity vector, and its effectiveness is proportional to the magnitude of the spacecraft velocity. I. e. given the kinetic energy, $U(t) = 1/2 V(t)^2$, (where $U(t)$ is the kinetic energy and $V(t)$ is the magnitude of the current spacecraft velocity), then the rate of change in the kinetic energy with respect to a change in the velocity is,

$$\partial U(t) / \partial V(t) = V(t) \partial V(t) \quad (1)$$

Understanding this point is crucial to designing an effective SOI strategy, because the spacecraft velocity changes rapidly during the Saturn encounter. After approaching the Saturnian system at 5.44 km/sec., the spacecraft velocity rises to 31.4 km/sec. at periapsis and then falls again in a symmetric fashion. The portion of this curve after periapsis is shown in Fig. 1.

To minimize the ΔV requirement then, the SOI should be centered around the spacecraft periapsis. (Note that if the SOI were delayed by just eleven hours beyond periapsis there would not be enough propellant in the tanks to reach the desired initial orbit period, much less to perform any tour of the Saturnian system.) In addition, a cleanup maneuver should be scheduled as soon as practical after the SOI. There are two approved science opportunities which impact the scheduling of the SOI and its cleanup maneuver.

1. The spacecraft will cross Saturn's ring plane 4 hours before and 4 hours after periapsis. These crossings are unique opportunities for particular types of science

observations. Centering the burn does not leave adequate time on either end to set up and take these ring plane observations. Thus the SOI should be moved somewhat, either earlier or later in time. Moving it earlier so that the burn ends at periapsis costs 50 m/sec in the nominal burn magnitude (which is only 2.5 % of the mission's ΔV budget).

2. A close flyby of the distant Saturnian satellite Phoebe is available on the way in to Saturn, but the resulting date of the Saturn encounter is July 1, 2004. For that date the periapsis is followed too closely by a period of poor communication with the spacecraft (superior conjunction), which forces the cleanup maneuver to be scheduled at least 16 days after periapsis. Figure 1 then shows that for any magnitude error made at SOI, the cleanup cost will be about ten times as great as the SOI error

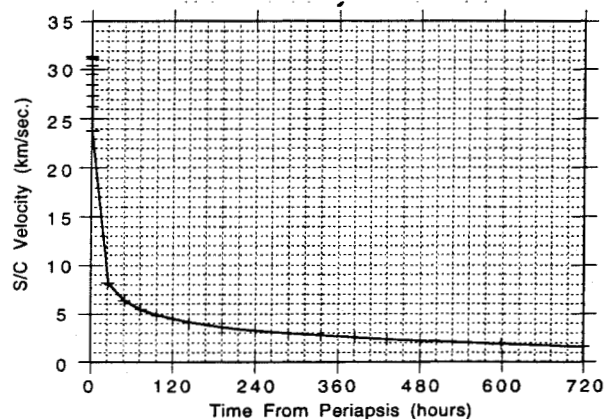


Figure 1 Spacecraft Velocity after Periapsis

The present plan is to end the SOI burn at periapsis and to target a first orbit period of 146 days (Ref. 1). This requires a ΔV of 620 m/sec and a burn time of 90 minutes. The time of periapsis on July 1, 2004 will depend on a choice by science to support the Phoebe flyby, but in the meantime a value of 08:40 GMT will be used.

Fault Tolerance Considerations for SOI

Because it is so important to complete SOI in the vicinity of periapsis, the operations team will transmit a sequence of commands to the spacecraft a few days prior to SOI, and will instruct the spacecraft to start executing these commands at an appointed time. Given the 160-minute

round-trip light time to Saturn, the operations team will not be able to assist the spacecraft in any meaningful way during the SOI burn. If a failure occurs prior to or during the SOI burn, the spacecraft must autonomously detect, locate and isolate that failure, autonomously restore any affected engine firing capabilities, and autonomously complete the necessary energy change.

Cassini carries a prime 440N engine and a backup 440N engine. The backup engine is isolated from its bi-propellants by a network of pyro-activated isolation valves and latch valves, and should remain that way for the entire mission. However, if the prime engine fails to perform at SOI, Cassini will be expected to autonomously unisolate the backup engine and use it to complete SOI.

The prime and backup 440N engines are physically adjacent to each other, and have not been qualified to perform "hot starts". After one engine fires for more than one second, that engine cannot be safely fired again for several hours, and the other engine cannot be safely fired for 45 minutes.

Given the previously described mission benefits of completing SOI prior to periapsis, the availability of a backup engine, and the cool down times between safe engine starts, the Cassini project developed the following strategy for responding to failures during SOI:

- 1) Once the SOI burn has started, respond to failures while continuing the burn if at all possible
- 2) If the SOI burn is terminated for any reason, cancel all science data collection and restart the SOI burn 45 minutes later, using the backup engine and an appropriately modified ΔV goal
- 3) If the SOI burn is terminated a second time for any reason, restart the SOI burn as soon as possible using the "best available" engine

Engine Failure Diagnosis: In order to support this strategy, Cassini's attitude control system must be able to autonomously verify that an engine is delivering acceptable

performance. Unfortunately, as is often the case in deep space flight systems, Cassini's engines are very lightly instrumented. The only sensor information available to the attitude control system is:

- a single-axis accelerometer that is approximately aligned with the thrust direction
- a single pressure sensor in the combustion chamber of each engine
- two temperature sensors in the combustion chamber of each engine

Since Cassini's engines are gimballed and also used for attitude control during engine firings, the attitude control system can also infer something about the engine performance from the performance of the attitude controller: if the attitude controller is stable, the engine must be delivering at least 1/3 of the expected thrust.

Table 1 is a summary of the attitude control system's diagnoses and responses to the available engine performance measurements during SOI. If an accelerometer measurement is available, it is classified as either Too High, OK or Too Low. If a pressure measurement is available, it is classified as either OK or Too Low. The two temperature measurements, if they are both available, are both used, and both must be higher than expected for the engine temperature to be declared Too Hot. By definition there is no engine pressure too high or temperature too low for the purpose of continuing the burn.

The toughest diagnosis is shown in the last line of the table, in which the accelerometer indicates the engine is not providing sufficient thrust, but the other sensor measurements are either unavailable or within the expected ranges. Is this an accelerometer failure or an engine failure? Although the symptoms here are somewhat ambiguous (i.e. it could just be an accelerometer failure), the burn cannot be allowed to proceed on a possibly faulty engine. Therefore the attitude control system must declare an "unconfirmed" engine failure. The response to this

Table 1: Autonomous Engine Failure Diagnosis During the SOI Burn

Acceleration	Engine Pressure	Engine Temperature	Attitude Controller	Continue the Burn?	Diagnosis
OK or NA	OK or NA	OK or NA	Stable	Yes	OK
OK or NA	Too Low	OK or NA	Stable	Yes	Pressure Sensor Failure
Too High	x	OK or NA	Stable	Yes	Accelerometer Failure
x	x	Too Hot	x	No	Engine Failure
x	OK or NA	OK or NA	Unstable	No	Engine Gimbal Failure
x	Too Low	OK or NA	Unstable	No	Engine Failure
Too Low	Too Low	OK or NA	Stable	No	Engine Failure
Too Low	OK or NA	OK or NA	Stable	No	Unconfirmed Engine Failure

Note: NA = Not Available x = Don't Care

diagnosis terminates the burn, declares both the prime engine and the accelerometer to be suspect, and restarts the burn on the other engine. The output of the now-suspect accelerometer will be ignored on the second burn attempt.

Engine Restart Decisions: If the SOI burn is terminated for any reason, the attitude control system must make two crucial decisions prior to a restart attempt. First, it must decide which engine to use for the restart attempt. Second, it must decide whether to impose a 45 minute wait time prior to the next attempt.

In selecting an engine for a restart attempt, the objective is simply to pick the engine that is safest and most likely to succeed on the next attempt. Table 2 outlines this decision, and the state variables that are used. The Prime Engine Temperature is an autonomously controlled state variable that can be either Hot or Cold, indicating whether the prime engine has actually been fired for more than one second in the past 24 hours. The Prime Engine Diagnosis is an autonomously controlled variable that can be either OK or Suspect, indicating whether the prime engine has ever been implicated in a previously failed SOI burn attempt. The Backup Engine Temperature and the Backup Engine Diagnosis provide similar information about the backup engine. Note that once an engine has been declared Suspect, it will not autonomously be reset to OK.

Table 2 illustrates the sequence of the decision tree. In line 1 the burn was aborted before the engine actually fired, so the prime is still fine, and switching is undesirable. But after the prime has been tried once and failed to fire, as in line 2, then it is marked as suspect, and the backup is tried the next time. In line 3, if the prime has been fired already then the backup is tried next, regardless of prime engine diagnosis. The last four lines show that if both engines are already Hot, then the one with the better Diagnosis is selected; if both engines are already Hot and have the same Diagnosis, then the default decision is to change engines.

These last four lines show increasing desperation, as both engines have already been fired. There is a dedication to

completing the SOI, in spite of some danger to the engine system. However if most of the burn has already been completed it brings up the topic of a Sufficiency Criteria, to be discussed below.

The decision to insert the 45 minute cool down delay is based on the above-mentioned Engine Temperature variables, as well as a single autonomously controlled boolean, called the Cool Down Delay flag. If both of the engines are Cold, then the flight software assumes the 45 minute delay is not necessary, and the Cool Down Delay flag is not even used. If either engine is Hot, then the flight software checks the Cool Down Delay flag. If the Cool Down Delay flag is False, then the flight software assumes this is the first restart attempt; it inserts a 45 minute delay, and then changes the Cool Down Delay flag to True. Once the Cool Down Delay flag has been asserted, it will not be autonomously cleared. If the Cool Down Delay flag is checked again later and found to be True, then the flight software will assume that this is at least the second restart attempt, and it will not insert another 45 minute delay in the SOI restart preparations.

Rotation of the Burn Direction: The spacecraft velocity vector rotates continuously as the spacecraft goes by its Saturn periapsis. Equation 1 then implies that for greatest efficiency the SOI maneuver must also rotate during the burn. The net gain from this during the nominal SOI is only 15 meters/sec., but can grow to over 100 meters/sec. if the burn restart is needed. As it happens, an SOI ending at periapsis is the most benign case for tracking the local spacecraft velocity vector by a constant rate of rotation. Figure 2 shows how well this design tracks the local velocity vector during and after the burn.

Not only does this burn track the spacecraft velocity well during the 1 1/2 hour burn, the fit is very good for a total of three hours after the burn start. This is plenty of time to handle any restart burn designed so far. If a further time modelling of the spacecraft velocity vector should need to be added, one possible option would be to define a new inertial

Table 2: Autonomous Engine Selection for an SOI Restart

Prime Engine Temperature	Backup Engine Temperature	Prime Engine Diagnosis	Backup Engine Diagnosis	Change Engines?	Rationale
Cold	x	OK	x	No	Prime still looks fine
Cold	x	Suspect	x	Yes	Prime must have failed to fire
Hot	Cold	x	x	Yes	Prefer cold engine to hot one
Hot	Hot	OK	OK	Yes	May as well change engines
Hot	Hot	OK	Suspect	No	Prime looks better than backup
Hot	Hot	Suspect	OK	Yes	Backup looks better than prime
Hot	Hot	Suspect	Suspect	Yes	May as well change engines

Note: x = Don't Care

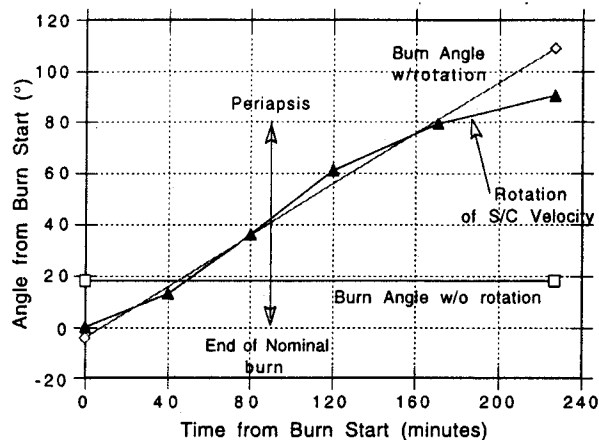


Figure 2
Constant Turn Rate Fit for SOI ΔV Direction

vector and rate polynomial starting at the end of a three hour period. However at this time the simple choice of a constant rate pitch turn during the burn (and afterward for some period of time) appears adequate for any expected anomaly response.

For implementing this time varying burn direction, trajectory plane coordinates are used, since the rotating spacecraft velocity stays within a plane during the Saturn encounter. These coordinates are fixed by the spacecraft position and velocity vectors at the burn start. The burn starts at -4.2° in right ascension, which means the burn direction lags the (rotating) spacecraft velocity vector by 4.2° at the start of the burn. The optimal burn direction rotation rate for this burn is 8.0 millidegrees/second.

The burn efficiency is less sensitive to accurate tracking of the velocity direction than might first appear. Any pointing errors in the SOI burn can be corrected later relatively cheaply, and possibly for zero cost by slightly adjusting the aimpoint for the next encounter. This leaves only errors in the magnitude to worry about, and the proportional loss in magnitude due to a pointing error of ϕ radians is given by

$$\text{loss} = 1 - \cos(\phi) \approx 1/2 \phi^2$$

Thus a steady pointing error of 6° would cause a loss in the desired burn magnitude of only half of one percent.

ΔV -to-go Calculation for Burn Restart: Some simple method is needed to specify the remaining ΔV needed after a burn stop and a 45 minute wait time before restarting. A third order polynomial fit was tried, with the resulting error curve shown in Fig. 3 below. The maximum resulting error was just 0.3 meters/second, which is about an order of magnitude smaller than the normal execution errors for this burn. Hence the third order polynomial was accepted as quite accurate.

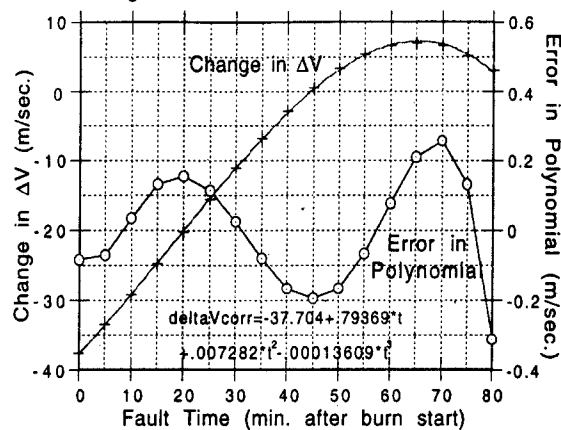


Figure 3
Third Order Polynomial Fit for SOI ΔV

If the SOI burn is terminated for any reason and then restarted after the 45 minute cool down period, the segmented burn will have a net change in ΔV as given in Fig. 3. Since the SOI ends at periapsis and the wait time is just half of the nominal SOI burn time, there is a net decrease in total ΔV cost for any interruption in the first half of the SOI. On any burn restart that follows the cool down delay, the attitude control system will adjust the ΔV -to-go as follows:

$$\Delta V\text{-to-go} = \Delta V\text{-commanded} - \Delta V\text{-measured} + (K_0) + (K_1)(T) + (K_2)(T^2) + (K_3)(T^3)$$

where:

- $\Delta V\text{-commanded}$ = the ΔV given in the ground provided burn command
- $\Delta V\text{-measured}$ = the ΔV measured in all prior burn attempts
- K_0, K_1, K_2, K_3 = constant coefficients
- T = the burn time prior to the 45 minute delay

When the attitude control system recalculates the ΔV -to-go, it checks for a negative ΔV -to-go, and if true declares SOI complete without initiating any additional engine starts. If the ΔV -to-go is positive but small it would be desirable to have a ground-provided "sufficiency criteria" to estimate when the benefits of completing the SOI aren't worth the risks of another restart attempt; again, the attitude control system would immediately declare SOI complete. Table 2 shows how desperate the engine risk can become with repeated unsuccessful restart attempts. In the next section the costs of not fully completing the SOI are discussed.

Sufficiency Criteria

The choice of a minimum sufficiency criteria for SOI is both complex and controversial. For example, stopping after 95% of the burn has been completed would leave a large net penalty of 280. meters/second to restore the original orbit period at the cleanup maneuver. This is equivalent to loss of about half of the planned Saturn tour. Future work will examine whether such a criteria could be made to depend on this not being the first attempt to do a restart, or on the total loss of the accelerometer. The possibility of not restoring the planned initial orbit period is discussed in the next section.

Acceptable Orbit: There is a heavy penalty in overhead associated with accepting a different orbit than the one chosen as nominal. A complete Saturn tour design will have been developed, based on a large commitment of time and effort. Even though the encounters with Titan which form the backbone of the tour could be shifted in 16 day increments (Titans' orbital period about Saturn), encounters with the smaller satellites (Icy Satellite encounters) would be lost.

If the period of the first orbit became very long, say more than a year or so, two other kinds of penalty would crop up. First, delaying the mission significantly would increase its dollar cost and make it harder to retain the best people through a long wait. Second, the orbit would become less stable, and perhaps require more control to fly. Of course the power supply would be slowly getting weaker as well, and other components of the spacecraft would have more time to degrade or even malfunction.

Early Emergency Maneuver

There is one more emergency backup preparation which can be carried out. If the SOI, in spite of the autonomous restart capability described above should come up substantially short, another emergency technique can be used. This is the Early Emergency Maneuver opportunity, scheduled 23 hours after the Saturn periapsis, when the energy penalty is only 2.7-to-one, instead of ten-to-one. A maneuver mini-sequence is developed ahead of time, with the spacecraft rotated so that the main engine thrust is pointed opposite to the spacecraft velocity vector. The only parameter to be inserted at the update is the magnitude of the burn ΔV . It takes 80 minutes for the radio signal to travel from Saturn to the Earth, but assuming some doppler data can be recovered soon after the SOI, an estimate can be made of how much more energy decrease is needed. The corresponding ΔV magnitude command is inserted into the mini-sequence and the sequence uplinked (another 80 minute delay) in time for this Early Emergency Maneuver.

Conclusion

Every possible means has been examined to ensure that the Cassini SOI will be successful. For that purpose

detailed plans have been developed for one or more autonomous restarts of the engine if needed.

Acknowledgment

This work was performed at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration.

Reference

1. Cassini Navigation Plan, JPL PD 699-506, May 29, 1996, pps. 4-55 to 4-59.

